Journal of Physics Communications

OPEN ACCESS

RECEIVED
8 May 2022

REVISED
24 May 2022

ACCEPTED FOR PUBLICATION
8 June 2022

PUBLISHED
11 July 2022



PAPER

# Differential-phase-shift quantum digital signature without disclosing measurement information

**Kyo Inoue**[1] **and Toshimori Honjo**[2]

[1] Graduate School of Engineering, Osaka University, Suita, Japan
[2] NTT Basic Research Laboratories, NTT Corporation, Atsugi, Japan

**E-mail:** kyo@comm.eng.osaka-u.ac.jp

**Keywords:** quantum digital signature, differential phase shift, quantum communication

## Abstract

A novel quantum digital signature (QDS) scheme using differential-phase-shift signal is presented. A sender broadcasts a weak coherent pulse train with 0 or $\pi$ phase to receivers, who measure its relative phases using delay interferometers with photon detectors and then employ the measurement results as authentication keys. The key distribution stage is completed with this signal transmission. Neither exchange of basis information between the sender and receivers nor exchange of a portion of a sifted key between the receivers with each other are conducted, unlike conventional QDS protocols. Therefore, our system is simpler than conventional ones. The security of the proposed scheme is discussed, and calculations evaluating system parameters to guarantee the QDS operation, such as the key length and authentication threshold, are presented.

## 1. Introduction

Quantum digital signature (QDS) has been investigated as a quantum communication technology. It guarantees the identity of a message sender and authenticates a digital message sent from a legitimate sender based on quantum mechanics. Since the first proposal of using a SWAP test and a quantum memory [1], several QDS protocols have been proposed, such as one using a multiport system configuration [2, 3], one utilizing quantum elimination measurement [4], and one based on quantum key distribution (QKD) [5].

In the above QDS protocols, the first two have technical issues for practical implementation. A quantum memory is required in [1, 2], which has not been realized in practice. In [2, 3], the signal transmission lines should be precisely controlled in terms of the propagation phase, the polarization state, and the temporal pulse position for perfect interference. In contrast, the third and fourth protocols utilize signal transmission systems similar to QKD, which is a mature technology in quantum communications. Especially, the fourth one directly relies on QKD systems, and has been primarily employed in experimental demonstrations [6–11].

In QKD-based QDS, a message sender and each recipient secretly pre-shared a bit sequence, i.e., a sifted key, using a conventional QKD system. After creating the sifted keys, the recipients exchange a portion of the sifted key with each other via a secured channel protected by QKD; the exchanged bits and the remainder of the originally created sifted key are maintained as a secret key to authenticate a signature key sent from the message sender. This scheme fully utilizes QKD technologies, and hence is the most implementable in QDS protocols. However, a number of QKD systems should be implemented; between a message sender and each recipient, and between recipients for secretly exchanging a portion of a sifted key. In addition, authenticated channels are used in QKD systems, and thus authenticated channels should be prepared for distributing authentication keys.

In order to reduce the number of physical transmission links, a measurement-device-independent scheme is employed in [8], wherein a central node (a message sender) is connected to two end nodes (message recipients), respectively. No additional link between recipients is required for the sifted key exchange in this scheme. However, the key exchange procedure is still performed, and the number of post-processing operations is not reduced.

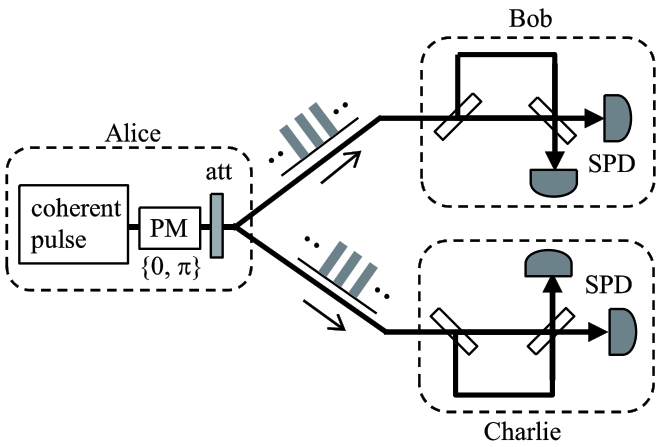


**Figure 1.** Setup of proposed DPS-QDS system. PM: phase modulator, att: attenuator, and SPD: single-photon detector.

Recently, a simplified QDS protocol was proposed, which has no bit exchange between recipients [12]. A sender alternatively sends nonorthogonal four states used in BB84-QKD to recipients. After the quantum transmission, the recipients disclose the photon detection time and the sender discloses the pulse intensity for a decoy method and ask the recipients to re-order the measurement results. The distribution of an authentication key is accomplished with these post-processing, eliminating bit exchange between recipients. However, some post-processing are still performed over authenticated channels, and thus authenticated channels should be prepared for distributing authentication keys.

Based on the above background, this study presents another QDS protocol featuring the simplicity. A message sender broadcasts a weak coherent pulse train with binary phases, that is similar to signal used in differential-phase-shift (DPS) QKD [13], to all recipients simultaneously, not alternatively as in conventional QDS protocols, which simplifies the signal transmission procedure. The recipients measure the signal similarly to DPS-QKD, from the result of which an authentication key is directly created at each recipient. No post-processing is conducted except that the sender alone discloses a portion of the modulation data for bit-error-rate (BER) estimation, which needs no authentication channel. This is because falsification of the sender's information by an eavesdropper just increases the BER and brings no benefit to the eavesdropper. In addition, the use of DPS signal simplifies the protocol, such that there is no measurement basis selection, a decoy method is not needed to beat the photon-number splitting attack [14], and the time domain is efficiently utilized.

In the following sections, the setup and operation of the proposed QDS protocol are presented, followed by discussions on the security issues such as robustness, forging, and repudiation. Subsequently, calculation examples of system parameters for satisfying the secured conditions are presented.

## 2. Protocol

### 2.1. Setup

The setup of the proposed DPS-QDS system is shown in figure 1. We assume three parties to demonstrate the basic QDS operation: Alice, who is to send a message, and Bob and Charlie, who are to receive Alice's message. In the distribution stage, wherein authentication keys are delivered from Alice to Bob/Charlie, Alice broadcasts a coherent pulse train to Bob/Charlie simultaneously. The pulses are phase-modulated by 0 or $\pi$, whose mean photon number is less than one per pulse (e.g., 0.1–0.2), similar to the signal transmitted in the DPS-QKD [13]. Bob/Charlie receives the pulse trains with a delay interferometer, followed by single-photon detectors. The delay time in the interferometer is equal to the pulse interval of the incoming pulse sequence, and the relative path phase of the two arms is 0. Subsequently, this system provides a measurement result to identify whether the phase difference of adjacent pulses is 0 or $\pi$, which is obtained occasionally and randomly because of the small mean photon number. Bob/Charlie records the time slots at which photons are detected and the measurement results of 0 or $\pi$ phase difference. Hereafter, a set of the time stamp and relative phase is regarded as a bit. Unlike the DPS-QKD, Bob and Charlie do not inform Alice regarding the time stamp, and hence no sifted bit is shared between Alice and Bob/Charlie and Alice does not know the recipients' bits.

### 2.2. Authentication/signature key

After the signal transmission mentioned above, Bob and Charlie, cooperating but not disclosing their bits with each other, select a sequence of pulses (e.g., from the $i$th to $j$th pulses) from Alice's pulse train and ask Alice to publicly disclose their phases. From the disclosed phases, Bob and Charlie individually extract phase differences that they measured, with which they estimate their bit error rates (BERs) and confirm if the estimated BERs have reasonable values expected from their receivers' performances. When the BER is notably higher than the expected value, eavesdropping against the transmitted signal or Alice's misbehavior of dishonestly sending pulses is suspected. Therefore, the above BER estimation checks if eavesdropping was conducted as well as if Alice honestly sent a pulse train to Bob/Charlie.

Subsequently to the above BER estimation, Bob/Charlie discard the measurement results used for the BER estimation, and maintain the remaining bits secretly as an authentication key. It is noteworthy that Bob's and Charlie's keys are partially identical but primarily different even though they received an identical pulse train from Alice; this is because the photon detection is occasional, random, and uncorrelated between Bob and Charlie. On the other hand, Alice discards the phase modulation data disclosed for the BER estimation and maintains the remaining bits secretly as her signature key. The length of Alice's key is considerably longer than that of the recipient's key created as mentioned above, because the mean photon number received by Bob/Charlie is less than one per pulse. The distribution stage is completed with the abovementioned DPS signal transmission followed by the BER estimation. There is no post-processing except that the Alice alone discloses a portion of the modulation data for bit-error-rate (BER) estimation. This Alice's information does not have to be sent through an authentication channel, because falsification by an eavesdropper just increases the BER, which provides no benefit to the eavesdropper. Moreover, the BER increment larger than a value expected from the receiver's performance suggests the eavesdropping.

A feature in the proposed scheme, different from the conventional QKD-based QDS protocol [5], is that Alice does not know the recipients' keys because the photon detection time is concealed in Bob/Charlie. Consequently, the recipients are not required to exchange half of their bits secretly to prevent Alice from knowing their keys, unlike the QKD-based QDS scheme.

In the message stage, Alice sends a message together with the signature key created in the abovementioned distribution stage. From this Alice's key, Bob/Charlie extracts the phase differences that he succeeded to measure in the distribution stage, and compares them with the measurement results. When a mismatch with Alice's key is identified at a ratio lower than a threshold value $s_a$, Alice's message is acknowledged as legitimate. Otherwise, the message is rejected.

## 3. Security

The security issues to be addressed in QDS are robustness, forging, and repudiation. In this section, we discuss these issues for our QDS protocol.

### 3.1. Robustness

In digital signature systems, the probability of receivers rejecting a message from the honest sender should be negligible small, e.g., less than $10^{-4}$. This criterion is known as robustness. In the present QDS protocol, the receivers estimate the BER in their keys in the distribution stage. Hereafter, we denote the estimated BER as $e$. The receivers reject Alice's message when they discover a bit mismatch ratio exceeding $s_a$ between the signature and authentication keys. Using Hoeffding's inequality [15], the upper bound of the probability of rejecting an honest message by Alice, $P$(honest abort), is expressed as follows [Appendix A]:

$$P(\text{honest abort}) = \Pr(s_a \geqslant e) \leqslant \exp\left[-2(s_a - e)^2 L\right], \tag{1}$$

where $L$ is the length of the authentication key. The system parameters, such as the authentication threshold $s_a$ and the key length $L$, are selected such that the upper bound of $P$(honest abort) is sufficiently small.

### 3.2. Forging

Forging in digital signature systems is an illegal action of a malicious party falsifying Alice's signature key and sending a fake message with it. The malicious party can be one of the receivers who created their keys in the distribution stage, e.g., Bob, who is the most formidable eavesdropper because he legitimately receives Alice's signal. Therefore, we considered the forging by malicious Bob cheating Charlie.

To perform forging, Bob must know Charlie's authentication key. He can legitimately obtain a fraction of it by measuring the signal sent from Alice to him. In particular, he measures Alice's signal immediately outside the site, as shown in figure 2, not at a distant position as in the normal condition. This is because the mean photon number per pulse received by Bob is highest at this position, providing him a large amount of the key

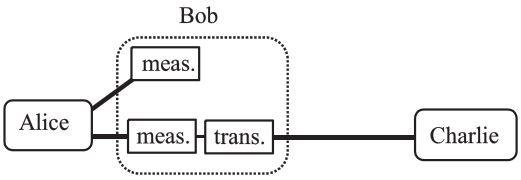


**Figure 2.** Bob's eavesdropping. Direct measurement immediately outside Alice's site and intercept-resend attack against transmission line from Alice to Charlie are conducted.

information. The probability of Bob knowing Charlie's key from this measurement is $\mu$ per bit, where $\mu$ is the mean photon number per pulse sent from Alice.

In addition to the above legitimate direct measurement, Bob can steal Charlie's key by attacking the transmission line from Alice to Charlie, as an eavesdropper (Eve) in QKD. In DPS-QKD systems, the general individual attack is often assumed [16], wherein Eve prepares a probe state with which Alice's signal state is entangled, stores the probe state, and then measures it based on the photon detection time disclosed by the receiver after the signal transmission. The use of the time information in the measurement can maximize the amount of information obtained through this eavesdropping. However, in the present QDS protocol, the detection time is not disclosed and cannot be utilized in measuring the stored probe state. Subsequently, eavesdropping schemes using a quantum memory are ineffective.

Therefore, malicious Bob conducts an intercept-resend (IR) attack, wherein he intercepts and measures Alice's signal, and resends a fake signal to Charlie according to the measurement result, as illustrated in figure 2. In particular, sequential IR attacks [17], which are formidable eavesdropping scheme against DPS signal, are launched. The amount of information stolen by this attack is not analytically expressed but can be numerically estimated [Appendix B].

Malicious Bob obtains a fraction of Charlie's key information through the direct measurement and the sequential IR attack against the transmission line from Alice to Charlie. We denote the probability of Bob knowing Charlie's key from these attacks as $\eta$ per bit in total.

Bob falsifies Alice's key based on his information regarding Charlie's key and sends it to Charlie with his fake message. Charlie compares the falsified key with his authentication key and acknowledges that the message is sent from Alice when the bit mismatch ratio is less than $s_a$. Bob's forging succeeds in this case. Here, Bob knows a Charlie's bit with a probability of $\eta$ owing to his eavesdropping; therefore, the bit mismatch probability between Bob and Charlie is $(1–\eta)/2$ per bit. Subsequently, the upper bound of the probability of Bob succeeding forging is expressed by using Hoeffding's inequality as follows [Appendix A]:

$$\begin{aligned} P(\text{forge}) &= \Pr(s_a \geqslant (1-\eta)/2) \\ &\leqslant \exp\left[-\{s_a-(1-\eta)/2\}^2 L\right]. \end{aligned} \tag{2}$$

Charlie selects the system parameters, $s_a$ and $L$, such that the upper bound of $P$(forge) is negligibly small (e.g., $10^{-4}$), to prevent Bob from forging.

### 3.3. Repudiation

Repudiation is an unfair action by malicious Alice, who contrives that her signature is accepted by a first recipient (e.g., Bob) but rejected by a second recipient (e.g., Charlie) to whom Alice's message is forwarded from the first recipient. Alice should create one signature key that is accepted and rejected by Bob and Charlie, respectively, for repudiation.

If Alice honestly sends a signature key based on her phase modulation in the distribution stage, then both Bob and Charlie will accept it owing to the robustness condition mentioned in section 3.1. Therefore, she flips some of the relative phases as $0 \rightarrow \pi$ and $\pi \rightarrow 0$ in her signature key to increase Charlie's bit mismatch ratio and lead him to reject the signature. However, Alice cannot intentionally select pulses for the phase flip because she does not know Charlie's photon detection time. Therefore, she randomly flips the relative phase with a ratio of $e_A$. Consequently, the bit mismatch probability between Alice's and the receivers' keys, both for Bob and Charlie, increases as $e + e_A – e \times e_A \approx e + e_A$ per bit.

Alice's foul key is compared with Bob's and Charlie's keys. Bob accepts and Charlie rejects Alice's key when the bit mismatch ratio is less than $s_a$ and larger than $s_v$, respectively, where $s_v$ is the authentication threshold for a forwarded signature key. Alice's repudiation succeeds in this case. Here, Bob simply forwards a signature key to Charlie with no operation on it, and subsequently, the bit checking processes at Bob and Charlie are independent with each other. Therefore, the success probability of repudiation is expressed as $P$(repudiation) $=$ $P$(Bob accept) $\times$ $P$(Charlie reject).

In the previous subsections, we evaluated the upper bound of the probability of a false operation (i.e., honest abort or forging) using Hoeffding's inequality to estimate the condition of the system parameters making the probability negligibly small. However, Hoeffding's inequality cannot be applied to $P$(repudiation) because the inequality yields the upper bound of the probability of a rare event, as shown in Appendix A, whereas Bob's acceptance probability is close to one. Therefore, we evaluated $P$(Bob accept) and $P$(Charlie reject) in an exact manner using a binomial distribution in the following.

A binomial distribution provides the probability that $n$ among $L$ bits are mismatched in the recipients' keys, under the condition that the bit mismatch probability is $e + e_{\mathrm{A}}$ per bit, as follows:

$$\Pr(n) = \binom{L}{n} \times (e + e_{\mathrm{A}})^n \times (1 - e - e_{\mathrm{A}})^{L-n}. \tag{3}$$

Bob accepts Alice's key when the number of mismatched bits is less than $s_{\mathrm{a}}L$, the probability of which is expressed as

$$P(\mathrm{Bobaccept}) = \sum_{n=0}^{s_{\mathrm{a}}L} \binom{L}{n} (e + e_{\mathrm{A}})^n (1 - e - e_{\mathrm{A}})^{L-n}. \tag{4}$$

On the other hand, Charlie rejects the forwarded signature key when the number of mismatched bits is larger than $s_{\mathrm{v}}L$, whose probability is expressed as

$$P(\mathrm{Charlie\ reject}) = \sum_{n=s_{\mathrm{v}}L}^{L} \binom{L}{n} (e + e_{\mathrm{A}})^n (1 - e - e_{\mathrm{A}})^{L-n}. \tag{5}$$

Note that, if Alice sent pulses partially different from those sent to Bob in the distribution stage, aiming at repudiation, the BER due to this Alice's misbehavior is taken into account in $e$ in equation (5). Using equations (4) and (5), the success probability of repudiation is expressed as

$$P(\mathrm{repudiation}) = \left\{ \sum_{n=0}^{s_{\mathrm{a}}L} \binom{L}{n} (e + e_{\mathrm{A}})^n (1 - e - e_{\mathrm{A}})^{L-n} \right\} \times \left\{ \sum_{n=s_{\mathrm{v}}L}^{L} \binom{L}{n} (e + e_{\mathrm{A}})^n (1 - e - e_{\mathrm{A}})^{L-n} \right\}. \tag{6}$$

Alice selects $e_{\mathrm{A}}$ to maximize $P$(repudiation). Charlie selects $s_{\mathrm{v}}$ such that $P$(repudiation) is negligibly small for any $e_{\mathrm{A}}$.

## 4. Calculation

We evaluated system parameters that guarantees the QDS operation for our proposed scheme. The system conditions assumed in the evaluation were based on the DPS-QDS experiment reported in [6]: the dark count rate and detection efficiency of a single-photon detector were 100 cps and 14% (including the filter loss in front of the detector), respectively, the bit error rate caused by imperfections of the interferometer was 1%, the fiber attenuation was 0.3 dB km$^{-1}$, the DPS pulse repetition frequency was 1 GHz, from which the pulse width was assumed to be 200 ps, and the mean photon number sent from Alice was 0.2 per pulse.

First, we evaluated the system parameters that satisfy the robustness condition using equation (1). The result is shown in figure 3, where the relationship between the receiver's key length and the authentication threshold, $L$ and $s_{\mathrm{a}}$ in equation (1), respectively, is plotted; the upper bound of $P$(honest abort) is $10^{-4}$. A longer key length and/or a higher threshold than the plot, i.e., the gray area in the figure, guarantees that the probability of honest abort is less than $10^{-4}$. The transmission distances between the sender and receiver were assumed to be 50 and 100 km, respectively. Although the calculation was performed for the two distances, the results obtained were almost identical and difficult to distinguish in the figure. This is because a photon detector with a low dark count rate was assumed in our calculations, and subsequently the receiver's BER, i.e., $e$ in equation (1), was dominated by the imperfection of the interferometer, which is independent of the distance.

Next, the system parameters for a negligibly small forging probability were calculated using equation (2). For the calculation, the eavesdropping probability $\eta$ should be evaluated. It comprises two components: the probability due to Bob's legitimate measurement (but at Alice's output) and that due to a sequential IR attack against the transmission line from Alice to Charlie. The former was estimated from Alice's mean photon number as $\mu$. The latter was evaluated as follows.

We first calculated the number of sequential successful measurements allowed for an eavesdropper, i.e., $k$ in Appendix B, which depends on the transmission distance. For the system conditions assumed herein, the number of allowable sequential measurements was numerically calculated as $k = 1$ for 0–10 km, 2 for 10–30 km, 3 for 30–55 km, 4 for 55–80 km, and 5 for beyond 80 km.

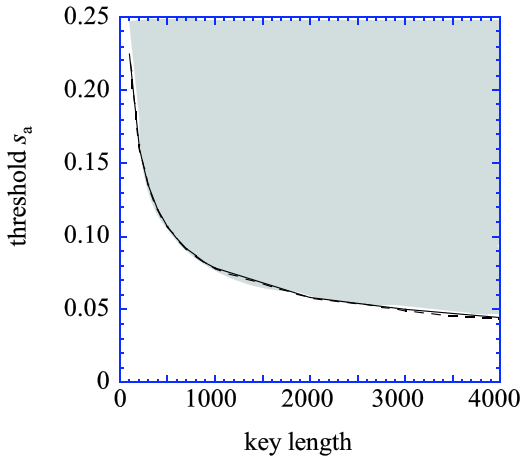


**Figure 3.** Receiver's key length and authentication threshold $s_a$ with which upper bound of probability of honest abort is $10^{-4}$. Gray area indicates the condition that the probability of rejecting a legitimate message is less than $10^{-4}$. Transmission distance between sender and receiver is 100 or 50 km, the upper bounds for which are denoted by the solid and broken lines, respectively. Both lines are almost identical and difficult to distinguish in the figure.

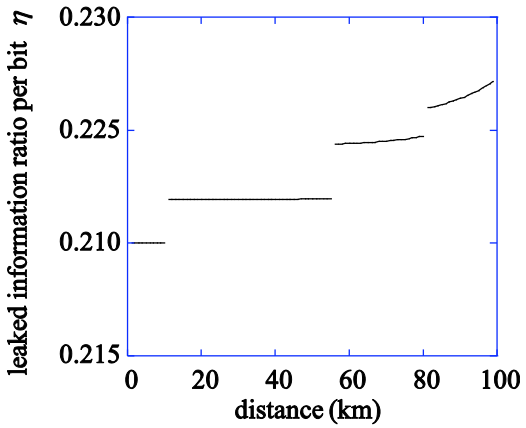


**Figure 4.** Probability of Charlie's bits being leaked to Bob as a function of transmission distance between Alice and Charlie. Bob is assumed to conduct legitimate direct detection and sequential intercept-resend attack against the transmission line from Alice to Charlie.

Next, we calculated the BER induced by the sequential IR attack, using the procedure described in Appendix B. The results were BER $= 0.25, 0.16, 0.12, 0.092$, and $0.076$ for $k = 1, 2, 3, 4$, and 5, respectively, which were obtained by optimizing the amplitudes of resent sequential pulses, i.e., $Aa_j$ in Appendix B. Subsequently, the probability of leaked key information as a function of the transmission distance was calculated, the results of which are shown in figure 4. The leaked information through Bob's legitimate direct detection was also included in $\eta$. A stepwise property was observed because of the discreteness of $k$.

Substituting the leaked information ratio $\eta$ obtained as above into equation (2), we calculated the key length $L$ and authentication threshold $s_a$, where the upper bound of the successful probability of forging was $10^{-4}$. The results are shown in figure 5, where the distances from Alice to Charlie were 50, 75, and 100 km. Parameter values below the plot can result in a forging probability of less than $10^{-4}$. For reference, the authentication threshold satisfying the robustness condition, shown in figure 3, is also plotted in figure 5. Based on this plot, the system parameters that prevent forging while satisfying the robustness condition can be obtained, as indicated by the gray area in figure 5.

Finally, we calculated the system parameters that prevented repudiation. The adjustable parameters for calculating the repudiation probability were the authentication threshold for the key directly received from Alice, i.e., $s_a$, the key length $L$, and the authentication threshold for a transferred key, $s_v$, as shown in equation (6). The former two parameters were determined from the requirements for robustness and forging, as shown in figure 5. Therefore, we considered the threshold $s_v$ for a transferred key for specified values of $s_a$ and $L$ determined from figure 5.

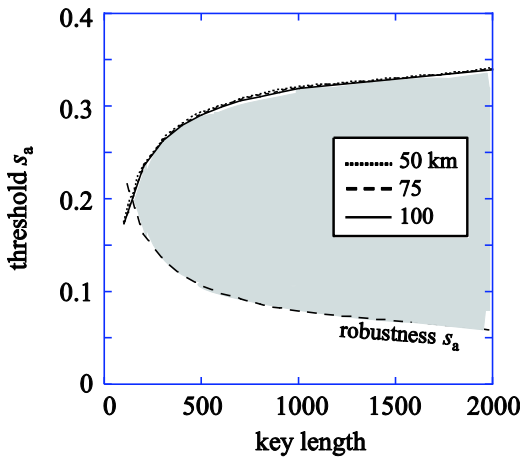


**Figure 5.** Receiver's key length and authentication threshold $s_a$, with which success probability of forging is $10^{-4}$. Transmission distance from Alice to Charlie is assumed to be 50, 75, or 100 km, the results for which are almost overlapped. Authentication threshold for robustness is also shown by broken line. Gray area indicates system conditions where the probabilities of forging successful and robustness unsatisfied are less than $10^{-4}$.

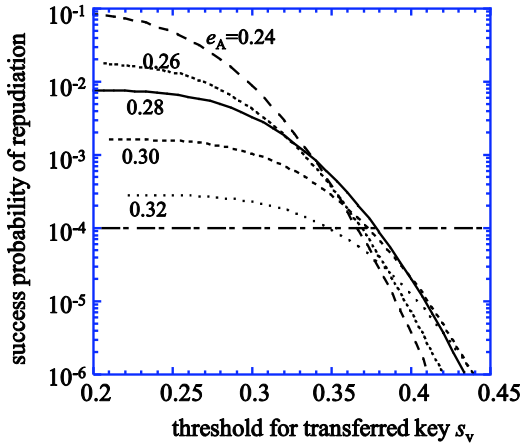


**Figure 6.** Success probability of repudiation as a function of authentication threshold, $s_v$, for transferred key. Transmission distance from Alice to Charlie was 100 km. Threshold for robustness was $s_a = 0.2$ and the key length was $L = 150$. Alice's intentional bit flip ratio was $e_A = 0.24, 0.26, 0.28, 0.30$, or 0.32.

Figure 6 shows the calculation results of the success probability of repudiation, $P$(repudiation), as a function of the threshold $s_v$, where the distance from Alice to Charlie is 100 km, the authentication threshold for Alice's direct key is $s_a = 0.2$, the receiver's key length is $L = 150$, and Alice's intentional phase flip ratio is $e_A = 0.24$, 0.26, 0.28, 0.30, or 0.32. It is observed that a flip ratio of $e_A = 0.28$ provides the highest threshold value for transferred key of $s_v = 0.38$ for the repudiation success probability to be $10^{-4}$. Therefore, the success probability of repudiation is less than $10^{-4}$ for any $e_A$ when $s_v$ is set at 0.38.

In figure 6, a flip ratio of $e_A = 0.28$ gives the highest threshold for a transferred key, although a threshold for a key gradually decreases with the error rate in general. The mechanism for this result is understood as follows. The success probability of repudiation is the multiplication of the probability of Bob's acceptance and Charlie's rejection, i.e., $P$(repudiation) = $P$(Bob accept) × $P$(Charlie reject), as shown in equation (6). For a small $e_A$, $P$(Bob accept) has a large value. On the other hand, $P$(Charlie reject) as a function of the threshold for a transferred key, $s_v$, behaves as shown in figure 7, which was calculated using equation (5). It is observed that $P$(Charlie reject) rapidly deceases with $s_v$ for a small $e_A$. Therefore, there is a trade-off in the behavior of $P$(repudiation), such that, as $s_v$ increases from a small value, $P$(repudiation) starts at a low level and slowly decreases for a large $e_A$ while it starts at a high level and rapidly decreases for a small $e_A$. As a result of this trade-off, there is a condition of $s_v$ for a given $P$(repudiation) being highest.

In the final of this section, we calculated the creation rate of an authentication key as a function of the signal transmission distance. First, the authentication key length for the secure QDS operation, $L$, was determined from the calculation results shown in figure 5. Next, Bob/Charlie's photon detection rate was calculated as

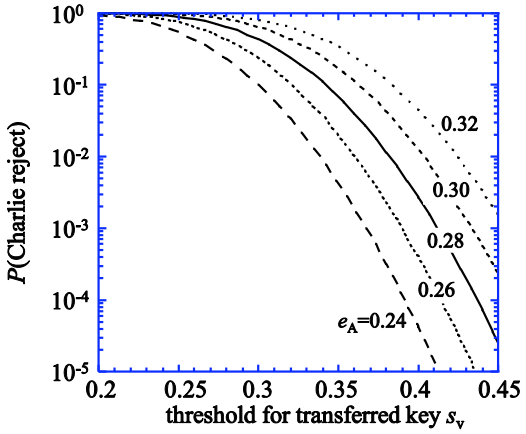


**Figure 7.** Probability of Charlie's rejection, $P$(Charlie reject), in the calculation shown in figure 6. Alice's intentional bit flip ratio was $e_A = 0.24, 0.26, 0.28, 0.30$, or 0.32.

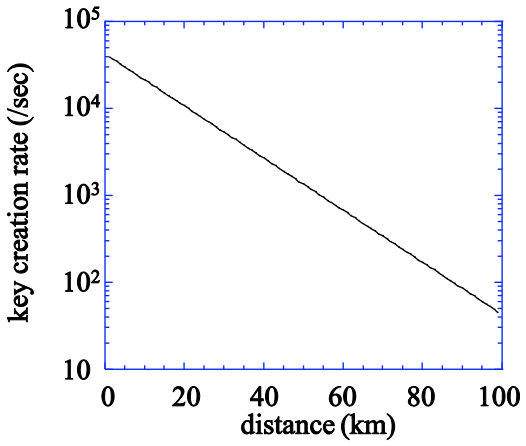


**Figure 8.** Key creation rate per sec as a function of transmission distance. The authentication key length and the test bit length are $L = 150$ and $2L$, respectively, for the probability of honest abort and the success probability of forging to be less than $10^{-4}$. The transmitter's mean photon number is $\mu = 0.2$ per pulse, the fiber attenuation is 0.3 dB km$^{-1}$, the transmittance of receiver's interferometer is $T_i = -2$ dB, the detector efficiency is $\eta_d = 14\%$, the pulse repetition rate is $R = 1$ GHz.

$N_d = \mu \times T_f \times T_i \times \eta_d \times R$ where $\mu$ was Alice's mean photon number per pulse, $T_f$ was the fiber transmittance dependent of the transmission distance, $T_i$ was the interferometer transmittance, $\eta_d$ was the detector efficiency, and $R$ was the pulse repetition rate. From the photon detection, binary bits were created, which would become authentication key bits and test bits for BER evaluation. Here, we assumed that the number of the test bits is twice the number of the key bits. Subsequently, the number of bits for creating one authentication key was $3L$, and the number of the created authentication keys was estimated as $N_d/3L$.

Figure 8 shows the calculation result of the key creation rate per second as a function of the transmission distance, where the parameter values in the DPS-QKD based QDS experiment [6] are assumed. It is noted that the key creation rate is proportional to the fiber transmittance $T_f$. The time to obtain one authentication key is given by the inverse of the key creation rate denoted by the vertical axis. In the present protocol, the DPS signal is broadcast to recipients simultaneously and there is no additional procedure after the signal transmission except for BER estimation, such as disclosing the measurement information and the pulse intensity (for a decoy method), and bit exchange or re-ordering, unlike conventional QDS protocols. Therefore, the consumed time for all recipients to obtain a final key is considerably shorter in the present protocol than in conventional protocols.

## 5. Summary

We proposed a DPS-QDS scheme without disclosing measurement information, which featured simplicity compared with conventional QDS protocols. DPS signal, which is a weak coherent pulse train with 0 and $\pi$

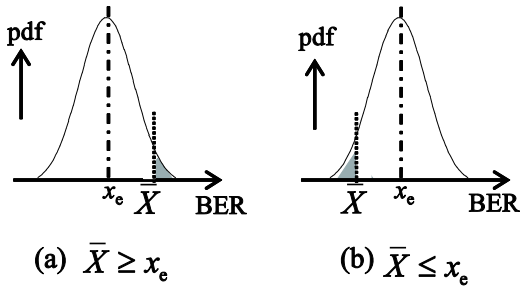


**Figure A1.** Probability distribution function (pdf) of bit error rate (BER). $x_e$ and $\bar{X}$ denote mean value and threshold, respectively. Gray area represents probability of interest.

phases, was broadcast to receivers simultaneously, who measured the signals using delay interferometers. The key distribution stage was completed with this signal transmission. Unlike the conventional QKD-based QDS protocol [5], no post-processing was performed, such as sifted-key sharing between the sender and each recipient, wherein the basis information is exchanged, and bit exchange between recipients, wherein the recipients firstly create a secret key via QKD and encrypt/decrypt exchanged bits with the shared secret key. Therefore, the present protocol is simpler than the conventional one.

The security issues, i.e., robustness, forging, and repudiation, for the proposed protocol were also discussed, assuming primitive eavesdropping, although a full security analysis against general attacks was not presented because this is the first proposal of a novel QDS protocol. Subsequently to the security analysis, calculation examples on system parameters to guarantee the QDS operation, i.e., the key length and the authentication thresholds, were presented.

## Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

## Appendix A

This appendix presents the method to apply Hoeffding's inequality to the present system. The original Hoeffding's inequality is expressed as follows [15]:

$$\Pr(\bar{X} - x_e \geqslant t) \leqslant e^{-2nt^2}, \tag{A1}$$

where the left-hand side denotes the probability of $\bar{X} - x_e \geqslant t$, $\bar{X}$ is the mean value of independent random variable $X_i$, i.e., $\bar{X} = (1/n)\sum_{i=1}^{n} X_i$, $n$ is the number of the variables, $x_e$ is an expected value of $\bar{X}$, and $0 < t < 1–x_e$. Equation (A1) is the original form of Hoeffding's inequality, from which we have

$$\Pr(\bar{X} \geqslant x_e) \leqslant e^{-2n(\bar{X}-x_e)^2}. \tag{A2}$$

Provided that we assign $X_i = 1$ or 0 when the $i$th bit in a bit-sequence is false or correct, respectively, $\bar{X}$ and $x_e$ are regarded as the bit error ratio in the bit sequence and the mean BER per bit, respectively.

In equation (A2), the probability is smaller for larger $(\bar{X} - x_e)$, which indicates that this inequality is for the case where $\bar{X} > x_e$, as illustrated in figure A1(a). Considering the symmetricity of a probability distribution function of the BER, the inequality can be applied to the upper bound of BER being below $\bar{X}$ when $\bar{X} < x_e$, as illustrated in figure A1(b). When we consider the threshold $s_a$ preventing honest abort, the probability profile of a BER is as shown in figure A1(a) with $x_e$ and $\bar{X}$ corresponding to $e$ and $s_a$, respectively. When we consider $s_a$ presenting forging, on the other hand, the probability profile of a BER is as shown in figure A1(a) with $x_e$ and $\bar{X}$ corresponding to $(1–\eta)/2$ and $s_a$, respectively.

## Appendix B

The sequential IR attack [17], which is an eavesdropping strategy assumed against our DPS-QDS, is described in this appendix. Against DPS signal, a simple IR attack, wherein an eavesdropper resends two isolated pulses based on the measurement result of the relative phase, induces bit errors when the legitimate receiver detects a photon at the edge time slots because of no interference occurring [13]. A sequential IR attack is designed to reduce this error by reducing the photon probability at the edge time slots.

In sequential IR attacks, an eavesdropper (Eve) intercepts the transmitted DPS signal, i.e., a weak coherent pulse train with 0 and $\pi$ phases, and measures its relative phases using a delay interferometer followed by photon detectors, similarly to a legitimate receiver. However, Eve cannot measure every phase difference because of a small number of photons in the pulse train. When Eve measures $k$ (or more) sequential phase differences, she resends a photon, through a lossless transmission line, super-positioned over $(k+1)$ sequential pulses with the measured relative phases. Otherwise, no resending is performed. Such a resent signal has a small photon probability at the edge pulses, thereby resulting in a small bit error rate.

The number of successful sequential measurements, $k$, is determined such that the number of photons received by a legitimate receiver is not changed via the eavesdropping. Under the normal condition, the receiver's photon number is $N\mu T$, where $\mu$ is the sender's mean photon number, $T$ is the transmittance between the sender and receiver, and $N$ is the number of pulses. On the other hand, the receiver's photon number under the sequential attack can be considered as follows. When the sequential attack is conducted, any sequence of $k$ pulses, such as $\{\#1$ to $\#(1+k)\}$, $\{\#2$ to $\#(2+k)\}$,…, $\{\#i$ to $\#(i+k)\}$, …, or $\{\#(N–k)$ to $\#N\}$ where $\#i$ indicates the $i$th pulse, possibly have one photon at the receiver. The number of the candidate sequences is equal to $N$ for $N \gg k$, and the probability of one sequence having one photon is equal to the probability of the sequential detections. Subsequently, the receiver's photon number under the sequential attack is (the number of pulses) $\times$ (the probability of sequential detections). Here, the probability of $k$ (or more) sequential detections by an eavesdropper at the transmitter output is expressed as $\Pr(0)\{\Pr(n \geqslant 1)\}^k$, where $\Pr(n)$ denotes the probability that $n$ photons exist in one pulse sent from the transmitter, and follows a Poisson distribution as $\Pr(0) = e^{-\mu}$ and $\Pr(n \geqslant 1) = 1–e^{-\mu}$.

When the sequential IR attack is partially conducted, for the BER induced by the attack to be small as described in the following paragraphs, the receiver's photon is $(1–r)\,N\mu T + rN\Pr(0)\{\Pr(n \geqq 1)\}^k$ where $r$ is the eavesdropping ratio. Eve should conduct the eavesdropping such that the receiver's photon number is not reduced from the normal transmission, the condition of which is expressed as

$$(1-r)N\mu T + rN\Pr(0)\{\Pr(n \geqslant 1)\}^k \geqslant N\mu T, \tag{B3}$$

from which we have

$$\Pr(0)\{\Pr(n \geqslant 1)\}^k \geqslant \mu T. \tag{B4}$$

Eve selects $k$ to satisfy this condition.

In resending $(k+1)$ pulses of one photon, Eve adjusts the amplitude of each pulse such that the photon probability at the edge pulses is further small, thereby resulting in a small error rate. This resent photon state $|\Psi>$ can be expressed as follows:

$$|\Psi> = A\left\{e^{i\theta_0}|0> + \sum_{j=-k/2, j\neq 0}^{k/2} a_{|j|}e^{i\theta_j}|j>\right\} \tag{B5a}$$

for even $k$ values, and

$$|\Psi> = A\sum_{j=-(k+1)/2, j\neq 0}^{(k+1)/2} a_{|j|}e^{i\theta_j}|j> \tag{B5b}$$

for odd $k$ values, where $|j>$ denotes the one-photon state at the $j$th pulse; $a_{|j|}$ and $\theta_j$ are the probability amplitude and phase of the $j$th pulse, respectively; and $A$ is a normalization constant to satisfy $A^2\Sigma a_{|j|}^2 = 1$.

The receiver measures the resent state with a delay interferometer, where one photon is detected at either one of $(k+2)$ time slots at the interferometer output, as illustrated in figure B1. A bit error can occur when a photon is detected at the first and last time slots because of no interference occurring. The photon probability at an edge pulse at the interferometer input is $\{Aa_{k/2}\}^2$ for even $k$, as indicated in equation (B5a), and that at an edge time slot at the interferometer output is $\{Aa_{k/2}\}^2/2$. Subsequently, the BER resulting from a photon detection at the edge time slots is $\mathrm{BER_{edge}} = \{Aa_{k/2}\}^2/2 \times 2 \times (1/2) = \{Aa_{k/2}\}^2/2$. In addition, the amplitude imbalance can cause a bit error in the interference between two neighboring pulses. The photon detection probabilities at two interferometer outputs are expressed as $A^2\{a_{|j+1|}{}^2 + a_{|j|}{}^2 + 2a_{|j+1|}a_{|j|}\}/4$ and $A^2\{a_{|j+1|}{}^2 + a_{|j|}{}^2 - 2a_{|j+1|}a_{|j|}\}/4$, and the BER due to the amplitude imbalance of the $(j+1)$th and $j$th pulses is expressed as $\mathrm{BER_{im}}(j+1, j) = (a_{|j+1|}–a_{|j|})^2/\{2(a_{|j+1|}^2 + a_{|j|}^2)\}$. Noting that the above BER resulting from each time slot, i.e., $\mathrm{BER_{edge}}$ and $\mathrm{BER_{im}}(j+1, j)$, includes the photon detection probability at each slot, the BER induced from a photon detection at either one of the time slots is the sum of each BER as $\mathrm{BER_{IR}} = \mathrm{BER_{edge}} + \sum_{j=-k/2}^{k/2-1}\mathrm{BER_{im}}(j+1, j)$. Eve chooses the amplitude of each pulse to minimize this $\mathrm{BER_{IR}}$. We carried out numerical calculations to find the optimal amplitudes for Eve to minimize the $\mathrm{BER_{IR}}$, the result of which is summarized in table B1.

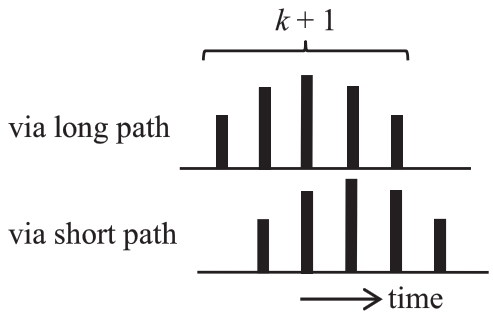


**Figure B1.** Pulse state at the delay interferometer output at a receiver when sequential IR attack ($k = 4$) is conducted. The upper and lower figures indicate pulses passing through long and short paths in the interferometer, respectively.

**Table B1.** Amplitudes of resent pulses and induced BER in optimized sequential IR attack.

| $k$ | Resent amplitudes | BER |
|---|---|---|
| 1 | $\sqrt{0.5}:\sqrt{0.5}$ | 0.25 |
| 2 | $\sqrt{0.307}:\sqrt{0.398}:\sqrt{0.307}$ | 0.16 |
| 3 | $\sqrt{0.219}:\sqrt{0.281}:\sqrt{0.281}:\sqrt{0.219}$ | 0.117 |
| 4 | $\sqrt{0.170}:\sqrt{0.215}:\sqrt{0.233}:\sqrt{0.215}:\sqrt{0.170}$ | 0.092 |
| 5 | $\sqrt{0.137}:\sqrt{0.169}:\sqrt{0.194}:\sqrt{0.194}:\sqrt{0.169}:\sqrt{0.137}$ | 0.076 |

Eve estimates the BER induced by sequential IR attacks as described above and partially conducts the eavesdropping with a ratio of $r = e/\mathrm{BER}_{\mathrm{IR}}$ where $e$ is the original system BER between the sender and receiver. From an intercepted-resent pulse sequence, Eve knows the receiver's bit probabilistically, but not deterministically. This is because the receiver detects one photon from the resent pulse sequence, the time slot of which is unknown to Eve. Under such condition, Eve supposes that the receiver creates a bit from the most likely two pulses in the sequence, i.e., the middle two pulses. The probability that the receiver counts a photon from the middle two pulses is $p_{\mathrm{m}} = A^2(1 + a_1^2)/2$ for a state expressed by equation (B5a) and is $p_{\mathrm{m}} = A^2(a_{-1}^2 + a_1^2)/2$ for that expressed by equation (B5b). Eve knows the receiver's bit with this probability for an intercepted-resent pulse sequence. Subsequently, Eve's eavesdropping probability in the sequential IR attack is given by $\eta_{\mathrm{IR}} = rp_{\mathrm{m}} = ep_{\mathrm{m}}/\mathrm{BER}_{\mathrm{IR}}$, which is evaluated from table B1 as $2.0 \times e$, $2.19 \times e$, $2.14 \times e$, $2.43 \times e$, and $2.55 \times e$ for $k = 1, 2, 3, 4$, and 5, respectively.

## ORCID iDs

Kyo Inoue https://orcid.org/0000-0001-5847-1727

## References

[1] Gottesman D and Chuang I arXiv: quant-ph/010532
[2] Clarke O, Collins R, Dunjko V, Andersson E, Jeffers J and Buller G 2012 *Nat. Commun.* **3** 1174
[3] Collins R, Donaldson R, Dunjko V, Wallden P, Clarke P, Andersson E, Jeffer J and Buller G 2014 *Phys. Rev. Lett.* **112** 040502
[4] Wallden P, Dunjko V, Kent A and Andersson E 2015 *Phys. Rev. A* **91** 042304
[5] Amiri R, Wallden P, Kent A and Andersson E 2016 *Phys. Rev. A* **93** 032325
[6] Collins R, Amiri R, Fujiwara M, Honjo T, Shimizu K, Tamaki K, Takeoka M, Sasaki M, Andersson E and Buller G 2017 *Sci Rep.* **7** 3235
[7] Yin H *et al* 2017 *Phys. Rev. A* **95** 032334
[8] Roberts G, Lucamarini M, Yuan Z, Dybes J, Comandar L, Sharpe A, Shields A, Curty M, Puthoor I and Andersson E 2017 *Nat. Commun.* **8** 1098
[9] Zhang C, Zhou X, Ding H, Zhang C, Guo G and Wang Q 2018 *Phys. Rev. Appl.* **10** 034033
[10] An X *et al* 2019 *Opt. Lett.* **44** 139–42
[11] Ding H, Chen J, Ji L, Zhou X, Zhang C, Zhang C and Wang Q 2020 *Opt. Lett.* **45** 1711–4
[12] Lu Y, Cao X, Weng C, Gu J, Xie Y, Zhou M, Yin H and Chen Z 2021 *Opt. Express* **29** 10162–71
[13] Inoue K, Waks E and Yamamoto Y 2003 *Phys. Rev. A* **68** 022317
[14] Inoue K and Honjo T 2005 *Phys. Rev. A* **71** 042305
[15] Hoeffding W 1963 *J. Am. Stat. Assoc.* **58** 13
[16] Waks E and Yamamoto Y 2006 *Phys. Rev. A* **73** 012344
[17] Tsurumaru T 2007 *Phys. Rev. A* **75** 062319